CERTIFICATE OF ELECTRONIC TRANSMISSION
I hereby certify that this correspondence is being electronically transmitted to United States Patent and Trademark Office on 28 January 2009.
/Kathryn Marley/
Kathryn Marley

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of Inventor:
Len L. Mizrah

Application No. **10/653,503**

Confirmation No. **3753**

Filing Date: **02 September 2003**

Title: **Key Generation Method for Communication Session Encryption and Authentication System**

Group Art Unit: **2439**

Examiner: **Farid Homayounmehr**

CUSTOMER NO. 22470

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

This Appeal Brief is filed in support of appellant's appeal from the Final Office Action in this case. A Notice of Appeal was filed electronically on 18 December 2008.

The appropriate fee as set forth in § 41.20 (b)(2) is being submitted herewith. Should it be determined that additional fees are required, the Commissioner is hereby authorized to charge those fees to Deposit Account No. 50-0869.

///

I. TABLE OF AUTHORITIES

Cases

II. TABLE OF CONTENTS

III. REAL PARTY IN INTEREST

The real party in interest is Authernative, Inc., the assignee of record.

IV. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

V. STATUS OF CLAIMS

All pending Claims 2-4, 6, 7, 9-11, 13, 14, 16-18, 20, 21, 31-39 are rejected. Claims 1, 5, 8, 12, 15, 19 and 22-30 were canceled prior to the filing of the notice of appeal. Claims 16-18, 20, 21, and 37-39 were canceled prior to filing the present brief. The rejections of pending claims 2-4, 6, 7, 9-11, 13, 14 and 31-36 are appealed.

VI. STATUS OF AMENDMENTS

An amendment canceling claims 16-18, 20, 21, and 37-39 was filed on 21 January 2009 under 37 C.F.R. §41.33(a). This amendment is pending.

VII. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claims 31and 34 are subject of the present appeal, and recite the same invention in method and apparatus categories, respectively. The subject matter of the independent claims is described with reference to the independent method claim 31.

The claims describe a method for mutual authentication in communications between first and second stations, such as the server 1001 and client 1003 in Figure 1. For the purpose of clarity in the following discussion, the first station is referred to as the server and the second station is referred to as the client. The invention provides for mutual authentication of the server and the client, without relying on previously distributed encryption keys and thereby reducing

administrative costs. Also, the invention provides for mutual authentication without sending shared secrets, such as passwords, neither in clear text nor in encrypted text, across the communication channel. Thereby the security of the protocol is improved.

The method includes generating and storing ephemeral session keys SRK1, SRK2, SRK3, ... (See reference numeral 1013 in Figure 1), and sets of intermediate data keys DRK1, DRK2, DRK3, ... (see reference numeral 2013 in Figure 2).

The server generates and stores a set of ephemeral session keys SRK1, SRK2, SRK3, ... (See reference numeral 1013 in Figure 1). Each of the ephemeral session keys is associated with a session key initiation interval, also called a "first lifetime LT1" (see, paragraph [0039]). Although not in claim 31, each ephemeral session key is described in the specification as having a second lifetime LT2 corresponding to the length of time that it remains in the server memory ASK 1013 before it is discarded (see, page 13, lines 16-30). The first lifetime LT1, referred to in the claims as the session key initiation interval, and its use are unique elements of the claims.

The server also generates and stores a set of intermediate data keys DRK1, DRK2, DRK3, ... The independent claim recites a single set of intermediate data keys. In the embodiment described in the application, unique sets of intermediate data keys 2013 are generated for each client session (reference numeral 2005, Figure 2).

According to the claimed method, the server responds to a request to initiate a communication session from the client by selecting the session key associated with the session key initiation interval during which the request is received (Figure 3, step 1, reference numeral 3005). Figure 1 shows requests (reference numerals 1006, 1015, 1016, 1017) made during the ninth minute, the fifth minute, the second minute, and the fifth minute, respectively. The requests fall within specific session key initiation intervals. The server selects the session keys in response to the requests, that are associated with the session key initiation interval in which the requests were made, for use in initiation of the requested session.

The associated session key is then sent to the client (Figure 3, step 2, reference numeral 3006), which returns a message carrying a digital identifier, such as a user name, encrypted using the associated session key (Figure 3, steps 3-4 (reference numeral 3007, 3008). The server is able to verify receipt of the associated session key and identify the client after decrypting the digital identifier carried in this message, and matching it with account records.

The server and client execute first and second sets of exchanges. The first set of exchanges results in delivery of an intermediate data key DRK1, or more generally DRK(n-1) to the client from the server (step numbers 4-5 (reference numerals 8000-8008) in Figure 8A). As stated in the specification, a larger number of exchanges utilized in the first set of exchanges results in greater security for the algorithm. However, for simplicity, we can refer to the results of the first set of exchanges as delivery of the first intermediate data key DRK1. The claims do not require the use of more than one intermediate data key in the first set of exchanges.

The second set of exchanges accomplishes mutual authentication using intermediate data keys up to DRK2, or more generally DRK(n), a first shared secret and a second shared secret (step numbers 6-9 (reference numerals 9000-8008) in Figure 8A). The first shared secret can be a client password (h-u-password). The second shared secret can be a server password (h-s-password).

Using the second set of exchanges, the server is able to authenticate the client and the client is able to authenticate the server by a process in which the first and second shared secrets are used for encrypting intermediate data keys. The shared secrets are not delivered across the communication channel. One way of using the shared secrets for the encryption of the intermediate data keys, for example, is shown at steps to 6-7 (reference numerals 8000-8008) on Figure 8A. In steps 6-7 (reference numerals 8000-8008) on Figure 8A, the server sends an intermediate data key DRK2, or more generally DRK(n), encrypted using intermediate data key DRK1, or more generally DRK(n-1), to the client. The client seeds a veiling algorithm (*e.g.*, Byte-VU, page 20, line 26 through page 21, line 7) using the client password (first shared secret) that is used in produce an encrypted version of intermediate data key DRK(n).

The hashed version of intermediate data key DRK(n), labeled h-DRK2 in Figure 8A, is returned to the server after encryption using the same intermediate data key DRK(n).

Therefore, the present invention provides a protocol for mutual authentication that is completely different than any in the prior art. Using this protocol, the first and second shared secrets need not be exchanged on the communication channel during the session. Also, using this protocol, no encryption keys need to be exchanged in advance of the session. Nonetheless, the server and client are mutually authenticated in a highly secure fashion.

VIII. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

(1) Whether claims 2-4, 6, 7, 9-11, 13, 14 and 31-36 are unpatentable under 35 U.S.C. §103(a) over Perlman (US 6,363,480), in view of Kelly (US 5,636,280), and further in view of Official Notice.

IX. ARGUMENT

In this case, the Examiner has made clear errors by misinterpreting the claims, by mischaracterizing the prior art, by relying on vague and improper Official Notice, and by failing to clearly articulate reasons for the rejection. The rejection should be reversed for these reasons.

The invention presented includes a combination of elements that provides a secure mutual authentication without previously shared encryption keys, that is completely different than any protocol in the prior art of record. Therefore, the invention as claimed is novel and non-obvious. The rejection should be reversed for this reason as well.

A claim is patentable under 35 U.S.C. §103, if the subject matter of the claim would have been nonobvious to persons having ordinary skill in the art. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966). The determination of patentability under 35 U.S.C. 103 has been based on several factual inquiries, including (1) the scope and content of the prior art, (2) the level of ordinary skill in the art; (3) the differences between the claimed subject matter and the prior art; and (4) secondary considerations of non-obviousness, such as commercial success, long felt but unsolved need, failure of others, and so on. Here, no evidence of secondary considerations is presented, because it is submitted that the first three factors, as discussed below, establish that the claimed invention would not have been obvious.

The analysis of these factors has been discussed in *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398 (2007) , and in the "Examination Guidelines for Determining Obviousness Under 35 USC 103 in View of the Supreme Court Decision in KSR International Co. v. Teleflex Inc.", Federal Register, Vol. 72, No. 195, pp. 57526-57535, issued by the United States Patent and Trademark Office on October 10, 2007 (the "USPTO Guidelines"). One overarching principle from *KSR* and the USPTO Guidelines on these issues is that "rejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *KSR* supra,127

S. Ct at 1741; quoted in USPTO Guidelines at 57528-57529. Applicant submits that no such reasoning has been set forth in the present record. Therefore, the USPTO has not met its burden of establishing obviousness and the rejections should be reversed.

In this case, the *prima facie* case relied upon by the Examiner can be characterized as a "picking and choosing" case. Specifically, elements set forth in the Office Action are chosen from the a number references that perform separate functions unrelated to the claimed invention, such elements are pieced together in a manner only possible in light of the present specification. The rejection in this case does not address all the claim limitations, but fills in the gaps by vague Official Notice, and misinterpretation of the references. The conclusion that the claims would have been obvious is presented based on these errors, without clear reasoning.

This "picking and choosing" case is rebutted herein by addressing misinterpretation of the claims and the references. In addition, the rejection is rebutted by highlighting the classic flaw in such reasoning. Specifically, the claims herein are non-obvious over this set of references because the claim elements in combination perform a function not found in the prior art, and "do not merely perform the function that each element [corresponding elements in the prior art chosen by the Examiner] performs separately." See, USPTO Guidelines, page 57534, at the end of the third column. Rather, the present claims provide a combination of elements which perform mutual authentication in a way that is completely different than the prior art, without relying on previous distribution of encryption keys and without relying on an exchange of shared secrets on the communication channel.

A. SCOPE AND CONTENT OF THE PRIOR ART

There are three elements of prior art officially relied upon in the Office Action, including Perlman, Kelly and a vague Official Notice. In addition, the Office Action cites Qi *et al*., the DES protocol and Schneier's Applied Cryptography in support of the Official Notice. Each of the references is summarized below to give an understanding of the scope and content of the prior art.

1. Perlman (US 6,363,480)

Perlman describes a problem that arises if an encrypted message is kept for a long period of time, and if the security of the encryption key that was utilized for encryption of the message

is weakened over time. For example, if an escrow arranged to maintain encryption keys over the long-term is compromised, the encryption keys might fall into the wrong hands, allowing an unintended person to decrypt messages that had been archived. Perlman, 1:59 through 2:4. To limit exposure to this problem, Perlman suggests the use of ephemeral encryption keys that are destroyed at an agreed-upon expiration date, beyond which messages encrypted using the ephemeral encryption keys cannot be recovered. The basic technique of Perlman involves a first party (the "ephemerizer") which provides a list of encryption keys with associated expiration times, and a second party which accesses the list, and selects an encryption key with an expiration time that meets its needs. Provided that the first party actually destroys the selected encryption key at the expiration date, and the first party does not disclose the selected encryption key to others, then the selected encryption key will not be available for decrypting the message after the expiration date.

Perlman also summarizes a protocol known as the Secure Sockets Layer (SSL) protocol at column 2, lines 19-27. The SSL protocol is mentioned here, because the Examiner appears to rely upon it in the Official Action. The SSL protocol involves a "forward secrecy" algorithm, utilizing layered encryption, in which a server maintains a long-term public/private key pair, and periodically generates short-term public/private key pairs. In setting up a communication, the client retrieves a short-term public key, which is authenticated using the long-term public/private key pair, and uses the short-term public key to encrypt a symmetric key. The symmetric key is shared with the server encrypted in this manner, and utilized for the session. When the short-term public/private key pair is discarded by the server, messages carrying the symmetric key in the session become unrecoverable.

Mutual authentication is not mentioned in Perlman.

2. Kelly (US 5,636,280)

Kelly describes a system for mutual authentication between a host computer and the remote computer based upon the use of a dedicated encryption key and encryption program provided in advance to both systems. The basic process of Kelly is described at column 7, lines 15-44.

In the process of Kelly, the remote computer makes an access demand to the host. The host is authenticated by the client if the client determines that an appropriate validating program

is running at the host. There is no discussion of how this determination is made for the purposes of authenticating the host in Kelly.

The host in Kelly identifies the dedicated encryption key of the remote computer using the client's user name or account number, provides an ephemeral "session key", and sends the session key to the remote computer encrypted using the dedicated encryption key. The remote computer decrypts the session key, and returns a password or a response to a challenge to the host, encrypted using the session key. Kelly refers to this algorithm as "reflexive" because, either the encrypted password, if a password is being used, or the encrypted response to a challenge, is returned to the host using the session key which had just been received from the host. Authentication of the remote computer is completed at the host by decrypting the password or the response and comparing it to an appropriate record available to the host.

In Kelly, mutual authentication depends on an unstated process for authenticating the server, on previously shared encryption keys, and on sending the encrypted user password or a response to a challenge across the communication channel. Therefore, it is fundamentally different than the present invention.

3. Improper Official Notice

This discussion is provided for the purposes of taking some position on the technology about which the Examiner has taken Official Notice. As discussed in detail below, the Official Notice is improper, and should be withdrawn.

The Official Action include the statement reading, "The nth and (n+1)th iterations also includes (sic) creating a hash of the session key, which the Examiner takes the (sic) Official Notice to be also a well-known technique in the art." (Official Action mailed 7 November 2008, Page 2, lines 18-20)

No claim uses the term “iteration.” No claim recites a process which can be interpreted as creating a hash of the session key, as the term "session key" must be interpreted in the present claims. There is no phrase in the claim that corresponds to the “nth and (n-1)th iterations.”

When the fact that the claim does not recite hashing a session key was pointed out to the Examiner, in the section of the Official Action entitled "Response to Arguments", the Examiner made a statement reading,

> Applicant further argues that the session (sic) is not

> hashed and it is actually the intermediate keys that are hashed. However, Examiner's Official Notice shows that hashing a session key is known in the art, which also shows that hashing a key is known in the art. In addition, what the applicant calls an intermediate key has a similar role as a session key. Meaning both keys represent a key that is valid temporarily, evidence (sic) by the fact that both the session keys and intermediate keys are discarded after they are expired.

(Official Action mailed 7 November 2008, Page 3, lines 8-13).

This position by the Examiner might be interpreted as modifying the Official Notice to refer to the intermediate key, which is subject of hashing in certain steps of the claim. However, such modification of the Official Notice would be inconsistent with the statement just above it on the same page reading, "Therefore, it is clear that the subject of Official Notice in said phrase is that creating a hash of a session key is known in the art." (Official Action mailed 7 November 2008, Page 3, lines 3-4). Now this restatement of the Official Notice leaves out the concept of iterations.

The Official Notice emphatically taken by the Examiner in the Office Action is not related to the claims herein in any coherent fashion. Nonetheless, the references cited by the Examiner in support of the Official Notice are summarized here as part of the scope and content of the prior art.

4. Qi et al.

The Examiner cites paragraph [0055] of Qi *et al.* (U.S. Patent Application Publication No. US 2003/0185391) to "reinforce the Official Notice." This paragraph includes the phrase

> The server 303 then performs a hash of the derived session key combined with the other information known to server 303 to verify the identity of the client 301. Similarly, at 335, server 303 sends a [hash of the session key] along with other information known to the client 301 to allow client 301 to verify the identity of the server 303.

In Qi *et al*., the "session key" is the key utilized for encryption during the session. It is unrelated to the "associated session key" of the claims herein. Likewise, it is unrelated to the intermediate data keys that are subject of hashing in the present claims.

5. Schneier, Applied Cryptography

At page 21, the Office Action refers to an algorithm called SKEY described on page 53 of the Schneier text. Apparently, this citation is also supposed to support the Official Notice.

SKEY is a one way authentication process based on a list of one-time passwords that the user carries around in her pocket. It does not involve hashing and it does not involve iterations. The Examiner states that this reference, "clearly teaches the concept of repeated application of a cryptographic technique to improve the security of the protocol." (Office Action, page 21, lines 7-8). This is clearly mistaken in reference to SKEY. In fact, the SKEY algorithm as described in the citation depends on giving the client a list of numbers in advance without any iterative distribution algorithm. Furthermore, the numbers in SKEY are used simply as one-time passwords. The protocol of their use is not described.

The Examiner also states that this reference "uses the hash function for the same purpose, *i.e.* using it to verify the integrity of exchanged data, *e.g.* session or intermediate keys." (Office Action, page10, lines 1-2). This comment is clearly mistaken. There is no hash function mentioned on page 53 in this reference. There is no exchange of hashed data mentioned in this reference.

6. DES

The DES protocol is referred to in the Office Action at page 22, lines 20-21, as follows: "Also use of a hashed version of a key is known in the art, as exemplified in DES protocol." DES is an encryption protocol, having nothing to do with the mutual authentication of the present claims.

B. DIFFERENCES BETWEEN THE CLAIMS AND THE PRIOR ART

The second component of the *Graham v. John Deere* patentability analysis is the difference between the claims and the prior art. In general, the present claims are fundamentally different than the prior art represented by the references in the record. No reference utilizes

ephemeral encryption keys like the session keys and intermediate data keys of the claims, produced at the server in the way claimed. No reference utilizes a procedure that provides mutual authentication without sending shared secrets such as passwords, across the communication channel in the way claimed. No reference accomplishes mutual authentication without previously distributed encryption keys.

The specific differences recited in the claims are identified and discussed in connection with the specific claims below.

C. LEVEL OF SKILL IN THE ART

The third component of the *Graham v. John Deere* patentability analysis is the level of ordinary skill in the art. The technological field of the present application is cryptographic authentication systems. The level of ordinary skill in this field is hard to quantify in a proceeding before the U.S. Patent and Trademark Office. Reference to the prior art cited can be made to reach some conclusions about the level of skill in the art.

On this record, the person having ordinary skill would have known about versions of SSL, DES and SKEY known in 2003, in addition to the references formally relied upon by the Examiner.

D. ISSUES OF CLAIM INTERPRETATION

It is fundamental that any *prima facie* case must be supported by a proper interpretation of the claims. See MPEP §2111. Claims should be interpreted in a manner that is both consistent with the claim language, and consistent with the specification. In this case, this fundamental requirement of consistency has not been met. The rejection should be reversed because it depends on a flawed interpretation of the claims.

For the purposes of this argument, we address three of the limitations in independent claims outlined below.

1. "session key initiation interval"

The phrase "session key initiation interval" is introduced in the first two clauses of independent claim 31 (claim 31, lines 3-7). These clauses require that ephemeral session keys be "associated with respective session key initiation intervals." Also, these clauses in claim 31

require that the associated session key, that is repeatedly referred to in the following steps in the claim, be selected in response to a request to initiate a communication session received during a particular session key initiation interval.

Therefore, the "session key initiation interval" in the claims refers to an interval of time during which the associated session key will be selected for use in the initiation of a communication session. The phrase should be interpreted in this manner.

The specification clearly defines a session key initiation interval, and distinguishes it from the time at which the session keys are discarded. In the example described in the specification, the session key initiation interval is labeled a first lifetime LT1, and distinguishes it from a second lifetime LT2 at which a session key is discarded, sometime after the session key initiation interval. See paragraphs [0039] – [0041].

The Office Action misinterprets "session key initiation interval," defining it instead so that it reads on the expiration time of the ephemeral key in Perlman. In Perlman, the expiration time is the time at which the keys are discarded and no longer available for use. See, Perlman, column 2, lines 58-61, and column 5, lines 22-25. This interpretation would be closer to the second lifetime LT2 described in the specification of the present application, defining the time that the session key is discarded from memory.

The claims specifically state that ephemeral session keys are "discarded at a time later than expiration of the respective session key initiation intervals." Therefore, the claims specifically distinguish the session key initiation interval from the time at which the session keys are discarded. The expiration time of Perlman corresponds to the time at which the keys are discarded, rather than to an initiation interval as required by the claim. Therefore, the Examiner's interpretation is inconsistent with the claim language and inconsistent with the specification.

In addition, the interpretation urged by the Examiner is inconsistent with claim 2 which discusses use of the same session key in response to another request received in the same session key initiation interval. Also, it is inconsistent under claims 4, 6 and 7, which specifically claim the session key lifetime as distinguished from the session key initiation interval.

As stated above, the broadest reasonable interpretation of "session key initiation interval" on the present record is an interval of time during which a request for access will result in selection of the associated session key for use in the initiation of a communication session. There

is no similar concept in the references of record.

When confronted with this interpretation, the Examiner stated:

> However, this is a trivial interpretation. As discussed above, if the key's session key initiation interval is the time during which the particular session key will be used for initiation of a session, then the interval does not begin unless the key initiates a session. This also applies to Perlman system. Even if Perlman selects a key based on its expiration time, whenever a key is selected, the session initiation key interval begins when the key initiates a session. Therefore, it reads on the claim requirement.

(Office Action, page 6). This quote reverses the specific claim language.

Taking the position, as the Examiner does here, that a session key initiation interval does not begin until a key is used to initiate the session, is not reconcilable with the claim language. The claims require the associated session key to be selected in response to a request received during the session key initiation interval. The claimed interval must begin therefore before or at the time the request is received. The Examiner's interpretation, defining the interval as beginning after the key is utilized, is contrary to the plain language in the claim.

2. "associated session key"

The phrase "associated session key" is also introduced in the first two clauses of independent claim 31 (claim 31, lines 3-7). The phrase is used repeatedly in the claims, preceded by the definite article "the". Fairly interpreted, the "associated session key" is the key that is selected based upon the session key initiation interval during which the request to initiate the session is received. It defines a particular session key that is selected in response to the request to initiate the session. It defines, in addition, the particular session key that is selected because it is associated with a particular session key initiation interval during which the request to initiate the session is received.

The Office Action reads "associated session key" on different things at different places. First, on page 17 lines 5-7, the associated session key is read on the key in Perlman that the second party selects from a list announced by the first party, where each key in the list is associated with an expiration time. As discussed above, a key associated with a "session key

initiation interval" as required in the claim is not fairly interpreted as a key associated with an expiration time.

In a second location at page 17, lines 15-19, the Office Action reads "associated session key" on some unspecified key utilized in the secure sockets layer SSL protocol which is briefly described in the background section of Perlman (Perlman, column 2 lines 19-34). The Examiner does not take a position on how the unspecified key utilized in the SSL protocol is an "associated session key" as required in claim. In fact, this portion of the Office Action omits the limitation "associated" when referring to this element of the claim.

In a third location at page 18, lines 4-9, the Office Action reads "associated session key" on a "session key" referred to in Kelly at column 7, lines 5-50. The "session key" described in Kelly is not related in any manner to a session key initiation interval.

In a fourth location, at page 19, lines 11-12, the Office Action apparently reads the "associated session key" on some element used for encrypting a digital identifier at column 7, lines 5-50 of Kelly. However, the algorithm of Kelly sends the identification number or account number, on which the digital identifier of the claims can be fairly read, without encryption (Kelly, column 7, lines 26-28). In Kelly, the user password is encrypted using an encryption key referred to as the "session key." However, as mentioned above, Kelly's session key is not similar to the "associated session key" the present claims.

Apparently, the Examiner is giving no weight to the claim language which requires that the associated session key be selected “in response to” receipt of the request to initiate a session “during a particular session key initiation interval.” This is a clear error.

The broadest reasonable interpretation of "associated session key" in the present claims is a particular session key selected in response to a request to initiate a session, and that is selected because it is associated with a particular session key initiation interval during which the request was received.

There is no concept similar to the "associated session key" in the references of record.

3. “intermediate data key”

The phrase "intermediate data key" is introduced in the fourth clause of claim 31, (claim 31, lines 14-16) and referred to repeatedly in following sections of the claim. The claim clearly distinguishes the intermediate data key from the associated session key, and states that they are

both discarded at some time later than expiration of the particular session key initiation interval, based upon which associated session key was selected. The specification clearly defines intermediate data keys DRK as distinct keys. In fact, Figure 1 is used to describe the generation of the session keys SRK, while Figure 2 is used to describe the generation of the intermediate data keys DRK.

The Office Action reads "intermediate data key" on the same key in Perlman as it reads "associated session key." It also uses the term "session key" as if it were interchangeable with "intermediate data key" in the claims. For example, at page 20, lines 10-20, the Office Action refers to its reading of "session key" on the ephemeral keys of Perlman. Apparently however, the Examiner is intending to address the limitations in claim 31 that relate to use of the "intermediate data keys" rather than the "session key".

The Examiner's interpretation of "intermediate data key" is internally inconsistent with the plain language of the claim, requiring that the "associated session key" be distinct from the "intermediate data keys." Furthermore, the Examiner's interpretation of "intermediate data key" is inconsistent with the specification.

The broadest reasonable interpretation of "intermediate data key," consistent with the claim language, and with the specification, is simply one of a set of keys generated at the server to be distinguished from the "associated session key," and utilized in the process as recited.

The rejection therefore should be reversed because it is based on flawed interpretation of the claims.

E. ANALYSIS OF SPECIFIC CLAIMS DEMONSTRATES THAT THE REJECTION SHOULD BE REVERSED

The present application includes two independent claims, including method claim 31 and apparatus claim 34 which are basically parallel in substance. Claims 2, 3, 4, 6, 7, 32 and 33 depend from claim 31, and claims 9, 10, 11, 13, 14, 35 and 36 depend from claim 34. These sets of dependent claims are also basically parallel in substance, differing in some cases because of the differing points of view of method and apparatus claims. We group the corresponding method and apparatus claims in the argument below.

1. Independent Claim 31 and Independent Claim 34 are patentable in view of the evidence in the record.

Independent method claim 31 distinguishes over the references in the record in at least five ways, addressed below.

a) Associated Session Keys

There is no algorithm in the prior art that involves session keys associated with session key initiation intervals, that are selected in response to a request to initiate a session, based on the particular session key initiation interval in which the request is received. See, claim 31, lines 3-7. The Office Action misinterprets the relevant clauses in the claims and mischaracterizes the prior art.

The Office Action reads claim limitation "in response to a request to initiate a communication session received by the first station during a particular session key initiation interval, selecting the associated session key" on column 6, lines 1-20 of Perlman (See Office Action, page 17, lines 4-7).

This is clearly wrong. In Perlman, the encryption key is selected based on a cognitive choice by the client, who reviews a list of available keys and their expiration times published by the server, and picks the key that has an appropriate expiration time. There is no selection in Perlman of a key associated with “a particular session key initiation interval". There is no selection in Perlman of a key “in response to a request … received … during a particular session key initiation interval" associated with that interval.

Furthermore, contrary to the implication of this reading of the claim on Perlman, the keys in the published list in Perlman are not associated with session key initiation intervals in any form.

Because the Office Action misinterprets the claim, and relies on this mischaracterization of Perlman, it should be reversed.

b) Exchange of digital identifier and associated session key

There is no algorithm in the prior art including an exchange in which the associated session key is delivered to a client, and the client’s digital identifier is returned to the server

encrypted using the associated session key. See, claim 31, lines 8-13. Here the Examiner misreads the references, and presents a rationalization that makes no sense.

The Office Action is not coherent with regard to this limitation of the claims. It reads this limitation on some aspect of the encryption key in Perlman, on some aspect of the SSL exchange summarized by Perlman and on an unspecified part of the protocol in Kelly.

The Office Action at page 17, reads the limitation (at lines 8-13 of claim 31), reading "the digital identifier being encrypted using said associated session key to verify receipt of the session key by the second station and to identify the second station or the user of the second station" on Perlman column 6, lines 21-35, combined with Kelly at column 7, lines 5-50. In this passage at column 6, lines 21-35, Perlman says that the key selected by the user is utilized for encryption of content in subsequent messages.

This reliance on Perlman is clearly wrong. In Perlman, authentication precedes delivery of the encryption key to the client. There would be no reason to send an encrypted version of the digital identifier to the server in this context.

The passage at column 7, lines 5-50 of Kelly, describing all the steps in the Kelly protocol, is relied upon to suggest that the content of one of the messages sent by Perlman using the selected encryption key could include a digital identifier. In Kelly, the digital identifier is exchanged to identify the client before the "session key" is provided. In fact, Kelly describes an algorithm in which the digital identifiers are sent without encryption. (Kelly, column 7, lines 26-28).

A second interpretation of the claim is presented in the Office Action based on discussion of the SSL protocol summarized in Perlman in this part of the Office Action, at page 17-18. However, Applicant is unable to decipher what the Examiner's point is in connection with that protocol. It does, as the Examiner asserts, involve some layers of encryption, with long term keys, short term keys and symmetrical keys. The SSL process is not tied to the claims in any coherent fashion, and is not similar to the claimed process. There is no digital identifier identified in the SSL protocol. There is no “associated session key” identified in the SSL protocol.

In a third interpretation at page 18 of the Office Action, the term “digital identifier” reads on the password of Kelly. The term “digital identifier” reads on an account number or a user name, but not on a password. An "identifier" is used to identify the client, as the claim states. A

password is used for authentication of the client. These are distinct functions as is well known in the art. Kelly sends the user password to the server encrypted using the "session key" of its process (Kelly, column 7, lines 33-37). This is done as part of the authentication of the client. It is not done "to verify receipt of the session key ... and to identify the [client] ..." as required in claim 31, lines 8-13. The three positions taken by the Examiner are all off point.

Because the Office Action relies on mischaracterization of Perlman and Kelly, it should be reversed. Because the features of Perlman, Kelly and the SSL protocol chosen by the Examiner to rationalize the rejection do not relate to mutual authentication in any form, the rejection should be reversed.

c) First Exchange of Messages

There is no algorithm in the prior art that includes the claimed "first exchange of messages" in which the server distributes to the client an ephemeral symmetric encryption similar to the intermediate data key of these claims (See, claim 31, lines 17-31).

Here the Examiner appears to read "intermediate data keys" on the ephemeral keys in the list published by the server in the Perlman reference (See, Office Action, page 19). This is the same interpretation as applied to the session keys in the claims. However, the claims clearly distinguish the two sets of keys as discussed above.

Claim 31 recites the execution of a first plurality of exchanges, "after verifying receipt of the session key by the first station…" at lines 18-21. The Office Action reads the limitations at lines 18-21 of claim 31 on Kelly, column 7, lines 5-50. However, there is no similar verifying step in Kelly. This is clear error.

Claim 31 also recites the characteristics of the messages in the first exchange of messages, and the result of delivering an intermediate data key from the server to the client.

The Office Action paraphrases the claim and suggests without any clear reasoning that it reads on Perlman, at column 5, line 55 to column 6, line 20. This passage in Perlman does not describe a similar exchange of messages, and does not describe an exchange of messages that is executed after verifying receipt by the client of the associated session key. This reliance on Perlman is clear error.

The Examiner states at page 20, "Perlman's teaching of ephemeral keys is for the purpose of substituting a key with another after the lifetime of the key is expired. Therefore, the session

keys are substituted with a fresh key after expiration of their lifetime." It is not clear how the Examiner relates this to the claim language. However, it clearly misreads the reference. The keys in Perlman's list of keys are intended for use in completely independent sessions by different parties. There is no substitution of "session keys" in Perlman.

The Office Action also characterizes the first set of exchanges as iteration. Applicant points out that the claim does not require iteration. Rather, it requires an exchange of messages carrying specific data. The claim uses the index semantic "(i)" to allow for a sequence of exchanges to cycle through a number of intermediate data keys. However, there is no requirement that more than one intermediate data key be used in the first set of exchanges.

Here, the Examiner takes Official Notice that, to the extent Applicant can determine, well known art includes creating a hash of a session key. However, this "Official Notice" does not address the specific limitations in the claims. There is no hash of a session key in the claims. The hash of the intermediate data key in the claim is encrypted using the same intermediate data key. No reference uses a similar step.

The Office Action at page 21 makes reference to the DES protocol, apparently in support of the Official Notice. The Examiner characterizes DES by saying that it "basically deploys a plurality of stages that scrambles the input data iteratively, and each iterative stage uses a different parameter (a key) to perform a different operation. The key in each stage is extracted from the previous stage." The DES protocol is an encryption process, and not related in any coherent fashion to the present claims.

The Office Action at page 21 makes reference to an algorithm called SKEY described on page 53 of the Schneier text. Apparently, this citation is also supposed to support the Official Notice. However, as discussed above, SKEY seems completely off point.

Because no reference describes a protocol including anything similar to the first exchange of messages recited in the claims, the rejection should be reversed.

d) Second exchange of messages

There is no algorithm in the prior art that includes the "second exchange of messages" in which the intermediate data keys and hashed versions of the intermediate keys are encrypted using the client password and the host password, to accomplish mutual authentication (See, claim 31, lines 32-58). Again, the Examiner does not address the specific limitations in the

claims.

The Office Action merely recites the claim language followed by the following parenthetical:

> (the second set of exchanges again involves an iteration process, similar to what is discussed above, with a difference of using a second shared secret in addition to the first shared secret, and using a hashed version of an encryption key to encrypt the key. However, using the second shared secret is again repeating the same process where the first shared secret was used. Also, use of a hashed version of a key is known in the art, as exemplified by the DES protocol.)

(Office Action, page 23).

This parenthetical statement mischaracterizes the claim language. The second set of exchanges is substantially different than the first set. In fact, there is no similarity in the content and no similarity in the purpose of the first and second exchanges.

Apparently the Examiner believes that the first and second exchanges of messages are shown by some unstated combination of the references in the record. This clearly fails to meet the standard of providing a clear articulation of the reasons for rejection.

Furthermore, the references in this record do not support the conclusion. Accordingly the rejection should be reversed.

e) Mutual Authentication

There is no algorithm in the prior art in which mutual authentication is accomplished using ephemeral symmetric encryption keys like the claimed intermediate data key produced at the server (See, claim 31, lines 56-60). On page 23 of the Office Action, the Examiner cites Kelly, at column 6, lines 57-62.

This passage of Kelly states:

> When, after using both the permanent and transitory keys, either pathway presents reflexively the encrypted identifying data to the host computer, the data is decoded and compared to the retained record thereof and a response is rendered.

Here Kelly is describing the last step of the flow chart in its Figure 4. It involves authentication of only the client.

Kelly states that authentication of the server is accomplished by "detecting by the remote computer presence of the validating program in the host computer" (See, Kelly, column 7, lines 17-19).

Claim 31 requires verification of "possession by the second station of the first shared secret" and verification of "possession by the first station of the second shared secret" during the second set of messages as specifically recited in the claim. The process of Kelly is not similar.

The discussion above concerning claim 31 applies with equal force to independent apparatus claim 34.

Because the Office Action does not address all limitations in the independent claims 31 and 34 in any coherent fashion, it should be reversed. Because the prior art of record does not support a finding of obviousness, the rejection should be reversed.

2. Claims 32 and 35 are patentable over the references of record

Claim 32 depends from claim 31 and recites the step of using a prearranged one of the intermediate data keys for encryption of the message indicating authentication referred to in claim 31. No reference mentions a message of that indicates mutual authentication in any form.

The Office Action rejects this claim with the rationale "encryption using a key such as key (n-1) was well known in the art at the time of the invention. The motivation to do so would be to secure the message by delivering it in ciphertext rather than clear text." This rationale for rejection suggests that the mere fact that it is desirable to encrypt a message proves that it is obvious to do so in the specific manner claimed.

The rejection is flawed because it does not address the specific limitation in the claim that requires the use of a prearranged intermediate data key, which had been used earlier for

another specific purpose. These limitations in the claim have been ignored in the rejection, and therefore the *prima facie* case is incomplete and flawed.

Claim 35 is the parallel apparatus claim and is patentable for the same reasons.

3. Claims 33 and 36 are patentable over the references of record

Claim 33 adds the step of using the intermediate data key as a symmetrical key for encryption during later communications. This brings up a unique element of the claimed invention, in that in addition to performing mutual authentication in a highly secure and efficient manner, the process acts as a technique for secure distribution of a symmetric encryption key.

The Office Action states "the purpose of establishing keys between parties of communication is encrypting the message for the purpose of confidentiality protection, or integrity protection" (page 23, paragraph 6.3). This comment is not a rationalization for a finding of obviousness.

No reference in the record describes distribution of symmetrical keys. Perlman says that, if symmetrical keys are used, they should be delivered in an unspecified secure manner (See US 6,363,480, col. 6, lines 17-20). Kelly distributes its symmetric "session key" by using a previously shared encryption key selected based on the identifying data for the client (col. 7, lines 26-31) unlike the claimed process. Therefore, the *prima facie* case for rejection of claim 33 is incomplete and flawed.

Claim 36 is the parallel apparatus claim and is patentable for the same reasons.

4. Claims 2 and 9 are patentable in view of the evidence in the record.

Claim 2 recites a characteristic of the session key initiation interval and the associated session key which is unlike anything in the prior art. The Examiner overlooks the fact that the session key is associated with the particular session key initiation interval, and selected based on that association. There is no similar process described in Perlman as discussed in detail above with respect to claim 31. Furthermore, the idea expressed in claim 2 of using the same session key for different communication sessions with different parties, because the request for initiation of the sessions occurred during the same interval of time is completely different than anything in the prior art. This also suggests the unique and inventive character of the process using the associated session key recited in these claims.

Claim 9 is the parallel apparatus claim, and is patentable for the same reasons.

5. Claims 3 and 10 are patentable in view of the evidence in the record.

Turning to claim 3, it depends from claim 2, and is patentable for the reasons mentioned above. Furthermore, it recites the step of associating a unique set of intermediate data keys with each session key. There is no similar step in the prior art.

In addition, the rejection is flawed because the Examiner reads the intermediate data keys on the set of keys presented in the algorithm of Perlman. The Examiner has not provided any explanation of how Perlman suggests using a key uniquely associated with another key. Furthermore, the keys described in Perlman are final encryption keys, not applied to any process similar to the claimed protocol. Therefore, the rejection is unsupportable and should be reversed.

Claim 10 is the parallel apparatus claim and is patentable for the same reasons.

6. Claims 4 and 11 are patentable in view of the evidence in the record.

Turning to claim 4, the rejection includes the following statement: "setting the lifetime such that it is usable after the set up period is completed is a obvious, logical and trivial choice. It is a trivial choice to choose the lifetime of session keys to be longer than the initiation interval because the initiation interval is part of the session" (page 25, paragraph 6.6). This comment demonstrates a fundamental error made by the Examiner. Specifically, in the analysis of the session key initiation interval in claim 31, the Examiner read the “session key initiation interval” on the expiration time of the keys in Perlman. With respect to claim 4, the Examiner is taking a position that the initiation interval is different than the lifetime. Any coherent rejection of these claims cannot have it both ways. In fact, the concept of an initiation interval that is associated with a session key used as claimed herein, is not found in Perlman or any of the references in the record.

Claim 11 is the parallel apparatus claim and is patentable for the same reasons.

7. Claims 6 and 13 are patentable in view of the evidence in the record.

Claim 6 depends from claim 4 and provides further definition of the session key lifetimes, distinguishing them from the initiation intervals. Thus, claim 6 is patentable for at least the reasons discussed above in connection with claim 4.

Claim 13 is the parallel apparatus claim and is patentable for the same reasons.

8. Claims 7 and 14 are patentable in view of the evidence in the record.

Claim 7 provides characterization of parameter for limiting the lifetime of a session key. It is patentable for at least the same reasons as claim 4, from which it depends, as discussed above. Also, the Office Action relies on the generic idea that the lifetime of a key must be long enough to accomplish its function. This generic idea provides no teaching whatsoever of a limit on the lifetime of the key as recited in claim 7.

Claim 14 is the parallel apparatus claim and is patentable for the same reasons.

F. THE REJECTION SHOULD BE REVERSED BECAUSE OF RELIANCE ON IMPROPER OFFICIAL NOTICE

As discussed in detail above, the Official Notice in this record is incoherent, and should be withdrawn. See, MPEP §2144.03 Reliance on Common Knowledge in the Art or "Well Known" Prior Art. Furthermore, the rejection should be reversed because of its reliance on the improper Official Notice.

G. SUMMARY

Applicant appeals to the Board to reverse the rejection of all claims in the present application because no reasonable basis for rejecting them has been provided, and because the evidence in the record proves that the claimed invention is in fact non-obvious.

The rejection as set out in the Office Action is based on picking and choosing specific pieces of technology in the prior art, attempting to piece them together in a fashion that results in the claimed invention, and then offering vague rationalization for the combinations of elements. This technique is flawed in the present case, because the claims present a protocol that accomplishes something that is completely new and unrelated to the individual pieces of technology that the Examiner relies upon. The completely new result stated in the independent claims is mutual authentication based upon keys that are produced at the server, and that are not previously distributed to the client and without sending shared secrets over the communication channel. No reference in the record accomplishes this result. No reference in the record even suggests that this result is possible.

X. CONCLUSION

Reversal of the rejection and allowance of the application are respectfully requested.

The Commissioner is hereby authorized to charge any fee determined to be due in connection with this communication, or credit any overpayment, to our Deposit Account No. 50-0869 (File No. AIDT 1005-1).

Respectfully submitted,

Dated: 28 January 2009

/Mark A. Haynes/
Mark A. Haynes, Reg. No. 30,846
Attorney for Applicant

HAYNES BEFFEL & WOLFELD LLP
P.O. Box 366
Half Moon Bay, CA 94019
Tel. 650.712.0340
Fax 650.712.0263

XI. CLAIMS APPENDIX

1. (canceled).

2. (previously presented) The method of claim 31, including using said associated session key in response to another request to initiate a communication session from a third station received by the first station during said particular session key initiation interval, and using other session keys from the set of ephemeral session keys after expiry of said particular session key initiation interval.

3. (previously presented) The method of claim 2, including associating a unique set of intermediate data keys with each session key.

4. (previously presented) The method of claim 31, including:

providing a buffer at the first station;

storing the set of ephemeral session keys in the buffer; and

removing session keys from said buffer upon expiry of respective session key lifetimes, said session key lifetimes being longer than the respective session key initiation intervals.

5. (canceled).

6. (previously presented) The method of claim 4, wherein the session key lifetimes have respective lengths longer or equal to a time required for verification of mutual authentication using said first and second sets of exchanges in expected circumstances.

7. (previously presented) The method of claim 4, wherein the session key lifetimes have respective lengths which are a multiple M times a time required for verification of mutual authentication using said first and second sets of exchanges in expected circumstances, where M is less than or equal to 10.

8. (canceled).

9. (previously presented) The apparatus of claim 34, including logic to use said associated session key in response to another request to initiate a communication session from a third station received by the first station during said particular session key initiation interval, and using other session keys from the set of ephemeral session keys after expiry of said particular session key initiation interval.

10. (previously presented) The apparatus of claim 9, including logic to associate a unique set of intermediate data keys with each session key.

11. (previously presented) The apparatus of claim 34, including

a buffer at the first station;

logic to store the set of ephemeral session keys in the buffer and to remove session keys in said set of ephemeral session keys from said buffer after expiry of the respective session key lifetimes, said session key lifetimes being longer than the respective session key initiation intervals.

12. (canceled).

13. (previously presented) The apparatus of claim 11, wherein the session key lifetimes have respective lengths longer or equal to a time required for verification of mutual authentication using said first and second sets of exchanges.

14. (previously presented) The apparatus of claim 11, wherein the session key lifetimes have respective lengths which are a multiple M times a time required for verification of mutual authentication using said first and second sets of exchanges in expected circumstances.

15-30. (canceled).

31. (previously presented) A method for mutual authentication in communications between first and second stations, comprising:

generating and storing a set of ephemeral session keys at the first station, ephemeral session keys in the set being associated with respective session key initiation intervals, and being discarded at a time later than expiration of the respective session key initiation intervals;

in response to a request to initiate a communication session received by the first station during a particular session key initiation interval, selecting the associated session key;

sending a message carrying said associated session key to the second station, and receiving a response from the second station including a digital identifier, the digital identifier being information shared between the first station and the second station, or between the first station and a user at the second station, the digital identifier being encrypted using said associated session key to verify receipt of the session key by the second station and to identify the second station or the user of the second station;

generating and storing, in the first station, a set of intermediate data keys, the set of intermediate data keys including intermediate data key (i), for i = 1 to at least n, and being discarded at a time later than expiration of the particular session key initiation interval;

executing a first set of exchanges including one or more exchanges with the second station, after verifying in said first station receipt of the session key by the second station by decrypting the digital identifier using the associated session key at the first station and positively matching the decrypted digital identifier against an existing entry in a stored list of authorized users, the first set of exchanges including

sending a message to the second station carrying intermediate data key (i) from said set of intermediate data keys encrypted using the associated session key for a first exchange in first set of exchanges and using the intermediate data key (i-1) for subsequent exchanges in the first set of exchanges,

receiving a response from the second station including a hashed version of intermediate data key (i) encrypted using intermediate data key (i), decrypting the hashed version of the intermediate data key (i), calculating a hashed version of intermediate data key (i) at the first station, and matching the calculated hashed version and the received hashed version of intermediate data key (i) to verify receipt by the second station of intermediate data key (i);

executing a second set of exchanges for mutual authentication after verifying in said first station receipt of the intermediate data key (n-1) by the second station, including

sending a first message carrying intermediate data key (n) encrypted using a hashed version of a first shared secret,

receiving a response from the second station carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the first shared secret, and decrypting the hashed version of the intermediate data key (n) , calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the second station of the first shared secret;

sending a second message carrying intermediate data key (n) encrypted using a hashed version of a second shared secret; and

if the second station sends a response to the second message, carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the second shared secret, after possession by the first station of the second shared secret is verified at the second station, the verifying being accomplished at the second station by decrypting the intermediate data key (n) from the second message using the hashed version of the second shared secret, calculating a hashed version of the intermediate data key (n), and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the first station of the second shared secret, then

receiving the response from the second station, and decrypting the hashed version of the intermediate data key (n) using the hashed version of the second shared secret, calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) at the first station to verify mutual authentication of the first and second stations; and

if mutual authentication is verified at the first station, then sending a message indicating successful authentication.

32. (previously presented) The method of claim 31, wherein said message indicating successful authentication carries a signal encrypted using intermediate data key (n-1) or using another prearranged one of said intermediate data keys (i).

33. (previously presented) The method of claim 31, including using intermediate data key (n) as a symmetrical key to encrypt data during post-authentication in communications between the first and second stations in the communication session.

34. (previously presented) A data processing apparatus, comprising:

a processor associated with a first station, a communication interface adapted for connection to a communication medium, and memory storing instructions for execution by the data processor, the instructions including

logic to receive a request via the communication interface for initiation of a communication session between a first station and a second station;

logic to provide for mutual authentication in communications between the first station and a second station, comprising:

generating and storing a set of ephemeral session keys at the first station, ephemeral session keys in the set being associated with respective session key initiation intervals, and being discarded at a time later than expiration of the respective session key initiation intervals;

in response to a request to initiate a communication session received by the first station during a particular session key initiation interval, selecting the associated session key;

sending a message carrying said associated session key to the second station, and receiving a response from the second station including a digital identifier, the digital identifier being information shared between the first station and the second station, or between the first station and a user at the second station, the digital identifier being encrypted using said associated session key to verify receipt of the session key by the second station and to identify the second station or the user of the second station;

generating and storing, in the first station, a set of intermediate data keys, the set of intermediate data keys including intermediate data key (i), for i = 1 to at least n, and being discarded at a time later than expiration of the particular session key initiation interval;

executing a first set of exchanges including one or more exchanges with the second

station, after verifying in said first station receipt of the session key by the second station by decrypting the digital identifier using the associated session key at the first station and positively matching the decrypted digital identifier against an existing entry in a stored list of authorized users, the first set of exchanges including

sending a message to the second station carrying intermediate data key (i) from said set of intermediate data keys encrypted using the associated session key for a first exchange in first set of exchanges and using the intermediate data key (i-1) for subsequent exchanges in the first set of exchanges,

receiving a response from the second station including a hashed version of intermediate data key (i) encrypted using intermediate data key (i), and decrypting the hashed version of the intermediate data key (i), calculating a hashed version of intermediate data key (i) at the first station, and matching the calculated hashed version and the received hashed version of intermediate data key (i) to verify receipt by the second station of intermediate data key (i);

executing a second set of exchanges for mutual authentication after verifying in said first station receipt of the intermediate data key (n-1) by the second station, including

sending a first message carrying intermediate data key (n) encrypted using a hashed version of a first shared secret,

receiving a response from the second station carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the first shared secret, and decrypting the hashed version of the intermediate data key (n) , calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the second station of the first shared secret;

sending a second message carrying intermediate data key (n) encrypted using a hashed version of a second shared secret; and

if the second station sends a response to the second message, carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the second shared secret, after possession by the first station of the second shared secret is verified at the second station, the verifying being accomplished at the second station by decrypting the intermediate data key (n) from the second message using the

hashed version of the second shared secret, calculating a hashed version of the intermediate data key (n), and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the first station of the second shared secret, then

receiving the response from the second station, and decrypting the hashed version of the intermediate data key (n) using the hashed version of the second shared secret, calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) at the first station to verify mutual authentication of the first and second stations; and

if mutual authentication is verified at the first station, then sending a message indicating successful authentication.

35. (previously presented) The apparatus of claim 34, wherein said message indicating successful authentication carries a signal encrypted using intermediate data key (n-1) or using another prearranged one of said intermediate data keys (i).

36. (previously presented) The apparatus of claim 34, including using intermediate data key (n) as a symmetrical key to encrypt data during post-authentication communications between the first and second stations in the communication session.

37-39. (canceled).

XII. EVIDENCE APPENDIX

Applicant is not submitting any evidence in this appendix.

XIII. RELATED PROCEEDINGS APPENDIX

There are no related proceedings.